REMARKS

Claims 1-13, 16-21, 24-34, 36, and 38-41 are currently pending in the subject application, and are presently under consideration. Claims 1-13, 16-21, 24-34, 36, and 38-41 are rejected. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

I. Rejection of Claims 1-13 and 16-19 Under 35 U.S.C. §103(a)

Claims 1-13 and 16-19 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,721,779 to Funk ("Funk") in view of U.S. Publication No. 2005/0027797 to San Andres, *et al.* ("San Andres") in further view of U.S. Patent No. 6,760,843 to Carter ("Carter"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

The Office Action notes that Funk does not teach the steps of broadcasting messages to the plurality of computers, such that each message is received at each computer, and filtering the broadcast messages at each computer according to the associated privileges of the user associated with each computer, such that a given message will be displayed only where the associated privileges of the user allow the message to be displayed, as recited in claim 1, but cites paragraph 0086 of the San Andres patent as providing a teaching of broadcasting and filtering messages. The cited paragraph and the preceding paragraph read as follows:

> Using the Explorer, **users can browse the content tree** 220 and can access the various content objects. **Various actions are available to the user** to reveal different levels of nodes. ....The particular actions which can be performed by a user **upon accessing a node** depend upon the user's access rights with respect to the node, which are stored within the access rights databases 152 on the security servers 150. **Access rights of users can advantageously be specified within the database on a single-user basis.**
>
> In accordance with one aspect of the present invention, the Directory Service only "shows" to each user those nodes that the user is authorized to access, or equivalently, those nodes to which the user has access rights. (In the

> preferred embodiment, the lowest level of access rights a user can have at a node is "viewer-only." A user with viewer-only level access rights at a node can view certain properties of the node, but cannot either modify the properties or open the corresponding service.) Thus, each user is provided with a filtered view of the actual content of the network 100, seeing only the icons of the nodes that the user is authorized to view or otherwise access. (San Andres, ¶¶0085-0086, emphasis added)

The San Andres publication teaches a distributed directory service for an on-line services network comprises multiple, separate services. A given user can have different access rights to information stored in the database, such that information at a given node that is not within the access rights of the user is not displayed to the user. But as this passage makes clear, the information at the distributed network is not broadcast to a plurality of users, but is instead accessed by individual users at the distributed network. There is no teaching or suggestion of broadcasting a plurality of messages to a plurality of computers. It is further submitted that San Andres does not teach filtering a broadcast message at the plurality of computers, as recited in claim 1. As stated in the above citation from San Andres, "Access rights of users can advantageously be specified *within the database* on a single-user basis." Accordingly, any filtering of the content of the distributed network occurs within the database associated with the distributed network, not at the level of the user's computer. Carter does not remedy these deficiencies. It is thus respectfully submitted that claim 1 is patentable over the cited art.

It is also respectfully submitted that even if San Andres did provide the required teaching, there is no motivation to combine Funk and San Andres in the manner recited in the Office Action. The Office Action states that it would be obvious to modify Funk to add broadcasting of messages to a plurality of computers and distributed filtering of the messages to "provide controlled access shared documents in a database among approved users by individually defining the scope of their access to the data contained therein..." It is respectfully submitted, however, that this objective can be achieved in a more straightforward fashion by simply controlling access to the data within the database at the database itself, without the need for broadcasting the data or filtering the data at the destination of the broadcast. Accordingly, it is unlikely that one

skilled in the art would seek to modify Funk in the manner described in the Office Action absent the teachings of claim 1.

The Office Action further admits that even a proposed combination of Funk and San Andres does not teach updating the one way encrypted password file at each of the plurality of computers, wherein updating the one way encrypted password file includes attaching a new master password file to a message at a computer accessible by a systems administrator or security officer, encrypting the message containing the new master password file using a private key and pass phrase available only to the systems administrator or security officer, transmitting the message to the plurality of computers, and decrypting the message at each computer *using a public key corresponding to the private key*. Carter is cited as providing this teaching, but it is respectfully submitted that Carter does not teach the decryption of a message containing a master password file using a public key corresponding to the private key.

In the Carter system, a new password can be provided to each of a plurality of remote systems to replace a current password. To this end, a private key associated with the user is encrypted with the old password to produce a first encrypted key, and the private key is encrypted with the new password to produce a second encrypted key. The encrypted keys are then provided to a remote system. The first encrypted key is compared to a current password encrypted key at the remote system. If they are identical, the current password encrypted key is replaced with the second encrypted key to update the remote system. The procedure can also be used to pass new encryption keys to a remote system. In a more specific example cited by the Office Action, the transmission to the remote system further includes a new private key for the user that is encrypted via a symmetric encryption key, which is itself encrypted by the old private key.

It is respectfully submitted that Carter does not teach or suggest transmitting a master password file to a plurality of computers. As recited in claim 1, a new master password file is provided to update an existing one way encrypted password file that "includes a plurality of user identifications, associated one-way encrypted passwords and associated privileges for each authorized user." Thus, the master password file of claim 1 should comprise user identifications,

one-way encrypted passwords, and privileges for a plurality of different users. A given transmission in Carter contains passwords only for a single user, with the user's current and new passwords used to provide encrypted versions of the user's private key. Accordingly, there is no master password file to be encrypted. Further, the only matter in Carter that is taught to be encrypted with a private key is the temporary symmetric key used to protect the new private key. Nothing specifically associated with the user is ever encrypted with a private key, although the user's private key is itself encrypted for transmission in the Carter system. It is thus submitted that the proposed combination of Carter with Funk and San Andres would not produce a system as recited in claim 1.

Turning to the claims depending from claim 1, the applicant asserts that each dependent claim has its own specific limitations and features that define patentable invention over the prior art. For the sake of brevity, the discussion of certain dependent claims will be omitted. In focusing the discussion on specific claims, a concession of the patentable distinctiveness of the others is not intended.

Claim 5, which depends from claim 3, recites spoofing the user into believing that access has been gained to the computer upon request of the systems administrator or security officer, wherein spoofing includes the presentation of false messages and information to the user.

None of the cited references discuss providing an unauthenticated user with false data in any form. The Office Action cites the following portion of Funk:

> As further illustrated by FIG. 2, the processor element 16 connects via a transmission path to the communication port 18. The communication port 18 can be an electrical circuit card assembly of the type conventionally used for interfacing a computer element with a communication channel, such as the communication channel 22. In one embodiment of the present invention the communication port 18 includes a modem for transforming electrical digital data signals into a format suitable for transmission over conventional telephone wires. Alternatively the communication port 18 can be a hard wired parallel computer interface of the type suitable for connecting a computer processing element such as host element 44 with a terminal interface such as the type as used by an ATM device. In the illustrated embodiment, the processing element 16 can include a second operating program stored in the program memory for directing the processing unit to operate the communication port 18 to transmit the challenge

> signal 26 via the communication channel 22 to the client element 46. The transmission of the challenge signal 26 can be responsive to an access request signal generated by the client element 46 and transmitted via the communication channel 22 and the communication port 18 to the processing element 16. However, it should be apparent to one of ordinary skill in the art, that other protocols and systems can be used for activating the transmission of the challenge signal 26 by the host element 44.
>
> The host element 44 further includes a comparator element 24. The comparator element 24 can be an electrical circuit card assembly constructed according to well known principles of electrical engineering, for comparing two large digital data signals and for determining a substantial identity between the two compared signals. In the illustrated embodiment, the comparator element 24 connects via transmission paths to the processor element 16 and the communication port 18. As further illustrated by FIG. 2, the comparator element 24 can further connect to the optional controller unit 42.
>
> The comparator element 24 can receive the key signal 30 generated by the processor element 16 and the response signal 28 received at the communication port 18 via the communication channel 22. The comparator element 24 compares the response signal 28 with the key signal 30 and generates a match signal 34 representative of a substantial identity between the response signal 28 and the key signal 30. (Funk, Col. 12, lines 20-64).

The cited paragraph describes the processing of the challenge signal at a processor associated with a central database, but there is no discussion of anything more than refusing to accept an incorrect password. The only data generated in the paragraph is the key, which is neither provided to the user nor misleading. The idea of providing false information to mislead an unauthenticated user is not suggested by this passage or any other portion of Funk. San Andres and Carter also fail to teach or suggest spoofing a user attempting to access the system. Accordingly, it is respectfully submitted that claim 5 is nonobvious and patentable over the cited art.

Claim 6, which depends from claim 3, recites disabling a computer system to prevent access by the user upon a request by the system administrator. Funk, San Andres and Carter, taken alone or in combination, fail to teach or suggest disabling a system upon one or more rejections of user provided authentication. As discussed above, Funk, San Andres, and Carter simply provide for the rejection incorrect passwords and do not teach or suggest further action in

response to multiple failed log-on attempts. The Office Action cites the following passage from Funk in rejecting claim 6:

> In a further alternative embodiment, the system 10 can include a processor 16 and a processor 20 that are adapted to implement a second randomizing operation that can add further security to the public communication channel. This second randomizing operation can include a response signal digest operation, such as an MD5 operation, that encrypts the response signal 28 to generate an encrypted response signal for transmission over a public communication channel. The server employs the same digest operation to encrypt the key signal 30 to generate an encrypted key signal and the comparator 24 compares these doubly encrypted signals. Both the client and the server can retain or exchange any common encryption keys or other data necessary for the selected digest operation. A match indicates that the client has met the server's challenge and the system 10 grants access to the client. (Funk, Col. 8, lines 47-63).

This passage simply describes a randomization process for the encryption keys used in the authentication process. There is no teaching of disabling a computer system in response to a request from a system administrator. Accordingly, it is respectfully submitted that claim 6 is nonobvious and patentable over the cited combination of Funk, San Andres, and Carter.

Claim 7, which depends from claim 6, recites deleting a plurality of files from the computer system upon a request by the systems administrator or security officer. None of the cited references discusses remotely deleting system files to prevent an unauthorized user from accessing them. The Office Action cites a passage within Funk, discussing the encrypted challenge and response process used in authenticating in a user. It is thus respectfully submitted that claim 7 is nonobvious and patentable over the cited art.

Claim 8, which depends from claim 1, recites displaying a request for reauthentication at the direction of a system administrator or security officer. Claim 9, which depends from claim 8, requires that this reauthentication will take the form of a displayed log-in screen having a position for entry of the user identification and password. The Office Action cites two passages in Funk describing an initial authentication procedure. The claims, however, recite a reauthentication process, requiring an already authenticated user to reenter a user identification and password just to maintain the present connection upon the request of a system administrator.

Neither of the cited references discusses such a reauthentication process. It is thus respectfully submitted that claims 8 and 9 are nonobvious and patentable over the cited references.

Dependent claims 2-13 and 16-19 depend directly or indirectly from independent claim 1. The applicant asserts that these claims are nonobvious and patentable for the reasons discussed above under claim 1 and for their own unique elements.

For the reasons described above, claims 1-13 and 16-19 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

II. Rejection of Claims 20, 21, 24-34, 36 and 38-41 Under 35 U.S.C. §103(a)

Claims 20, 21, 24-34, 36 and 38-41 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Funk in view of San Andres in further view of U.S. Patent No. 5,289,540 to Jones ("Jones"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claim 20 recites a system to administer access and security on a network having a plurality of computers. The system includes a one-way encrypted password file on each computer of the plurality of computers in the network. The one-way encrypted password files include a plurality of user identifications, associated one-way encrypted passwords, and associated privileges for each authorized user allowed access to the plurality of computers and the network. A user login module receives a user identification or role and password from a user and logs in the user when a match is found in the one-way encrypted password file. A channel monitoring and filtering module monitors and receives broadcast or multicast messages within the network and displays the message to the user when the user's associated privileges permit the viewing of the message. A remote auditing module is operative to monitor and process anomalous events which may occur on the computer. The anomalous events comprise a change in the users' associated privileges, a system disable operation initiated by the user, the expiration of a user's password, the rejection of a message due to an invalid digital signature, a request for remote user re-authentication received from the systems administrator or security officer, a request for a remote user lockout received from the system administrator or security officer, and

successful completion of a request for remote loading passwords to a system administrator or security officer.

None of the cited art teaches or suggests the filtering and display of broadcast or multicast messages based upon user privileges, either alone or in combination. The Office Action notes that Funk does not teach this element, but cites a portion of the San Andres patent (¶0086) as providing the required teaching. It is respectfully submitted, however, that the required teaching is not present in San Andres, and that no motivation is present to modify Funk in the manner described. This is presented in detail in the discussion of claim 1, above.

Funk and San Andres, taken alone or in combination, also fail to teach or suggest a remote auditing module operative to monitor and process anomalous events, including a change in a users' associated privileges, a system disable operation initiated by the user, the expiration of a user's password, the rejection of a message due to an invalid digital signature, a request for remote user re-authentication received from the systems administrator or security officer, a request for a remote user lockout received from the system administrator or security officer, and successful completion of a request for remote loading passwords to a system administrator or security officer. The Examiner admits that neither Funk nor San Andres provide such a teaching, but cites a file security system in Jones as providing a teaching of the remote auditing module. It is respectfully submitted that the file security system of Jones does not teach or suggest the cited module.

The file system of Jones monitors a computer system for a number of events, including corruption in key processes and files on a computer and repeated, unsuccessful attempts to log on to the system (*See* Fig. 4). Jones does not teach or suggest a module that is operative to monitor for even one of the events recited in claim 20. The Office Action cites Fig. 4 and its related text as providing this teaching, but the cited figure does not provide the required teaching. There is no related text directly associated with the figure that might serve to provide additional teachings. (*See* Jones, Col. 10, lines 62-63). Accordingly, it is respectfully submitted that Jones does not teach the cited module and that claim 20 is patentable over the cited art.

Claim 31 recites a computer program executable by a computer and embedded in a computer readable medium to administer access and security on a network having a plurality of computers. A one-way encrypted password file is provided on each computer of the plurality of computers in the network. The one-way encrypted password file includes a plurality of user identifications, associated one-way encrypted passwords, and associated privileges for each authorized user allowed access to the plurality of computers and the network. A user login code segment receives a user identification or role and password from a user and logs in the user when a match is found in the one-way encrypted password file. A channel monitoring and filtering code segment monitors and receives broadcast or multicast messages within the network and displays the message to the user when the user's associated privileges permit the viewing of the message. A remote control code segment enables a system administrator or security officer to take appropriate action when an anomalous event transpires. The appropriate actions include the act of spoofing the user into believing that the access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user.

As discussed above under claim 1, Funk in view of San Andres does not teach or suggest the filtering and display of broadcast or multicast messages based upon user privileges, taken alone or in combination. In addition, the cited art does not teach or suggest a remote control code segment operative to allow a system administrator or security officer to spoof a user into believing that access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user. None of the cited references discuss providing an unauthenticated user with false data in any form. The Office Action cites a portion of Funk describing the processing of the challenge signal at a processor associated with a central database, but there is no discussion of anything more than refusing to accept an incorrect password. Neither Jones nor San Andres remedies this deficiency. The idea of providing false information to mislead an unauthenticated user is not suggested by this passage or any other portion of Funk. Accordingly, it is respectfully submitted that claim 31 is nonobvious and patentable over the cited art

Turning to the claims depending from claims 20 and 31, the applicant asserts that each dependent claim has its own specific limitations and features that define patentable invention over the prior art. For the sake of brevity, the discussion of certain dependent claims will be omitted. In focusing the discussion on specific claims, a concession of the patentable distinctiveness of the others is not intended.

Claims 25 and 36, which depend from claims 24 and 31 respectively, recite, when read in the context of the claims from which they depend, a remote control module operative to allow a system administrator or security officer to disable the computer system so that the user cannot access the computer system and delete a plurality of files stored in the computer in response to an anomalous event. None of the cited art teaches or suggests deleting a plurality of files from a system in response to an anomalous event. The Office Action cites a passage within the Funk, discussing the encrypted challenge and response process used in authenticating in a user. There is nothing in the cited passage that teaches the deletion of system files in response to an anomalous event. Neither San Andres nor Jones remedy this deficiency. It is thus respectfully submitted that claims 25 and 36 are nonobvious and patentable over the cited art.

Claim 26, which depends from claim 24, recites, when read in the context of the claim from which it depends, a remote control module operative to allow a system administrator or security officer to spoof a user into believing that access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user. None of the cited references discuss providing an unauthenticated user with false data in any form. The Office Action cites a portion of Funk describing the processing of the challenge signal at a processor associated with a central database, but there is no discussion of anything more than refusing to accept an incorrect password. Neither Jones nor San Andres remedies this deficiency. The idea of providing false information to mislead an unauthenticated user is not suggested by this passage or any other portion of Funk. Accordingly, it is respectfully submitted that claim 26 is nonobvious and patentable over the cited art.

Claim 34, which depends from claim 33, recites, when read in the context of the claim from which it depends, a remote auditing module operative to monitor and process anomalous

events, including a change in a users' associated privileges, a system disable operation initiated by the user, the expiration of a user's password, the rejection of a message due to an invalid digital signature, a request for remote user re-authentication received from the systems administrator or security officer, a request for a remote user lockout received from the system administrator or security officer, and successful completion of a request for remote loading passwords to a system administrator or security officer. In the stated reasons for rejection of claim 20, the Examiner admits that neither Funk nor San Andres, taken alone or in combination, provide such a teaching, but cites a passage in Funk in rejecting claim 34. (See Office Action of July 05, 2005, pg. 10, lines 10-18). The withdrawal of this rejection is respectfully requested as Funk, by the Examiner's own admission, does not contain the stated teaching. Further, it is respectfully submitted that Jones does not teach or suggest the cited code segment, for the reasons discussed above under claim 20. Accordingly, claim 20 is nonobvious over the cited art.

Claims 28 and 39, which depend from claims 20 and 31, respectively, recite displaying a request for reauthentication at the direction of a system administrator or security officer. The Office Action cites two passages in Funk describing an initial authentication procedure. The claims, however, discuss reauthentication, requiring an already authenticated user to reenter a user identification and password just to maintain the present connection upon the request of a system administrator. Neither San Andres nor Jones remedy this deficiency. It is thus respectfully submitted that claims 28 and 39 are nonobvious and patentable over the cited references.

For the reasons described above, claims 20, 21, 24-34, 36 and 38-41 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested

CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 3/23/06

Christopher P. Harris
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
526 SUPERIOR AVENUE, SUITE 1111
CLEVELAND, OHIO 44114-1400
Phone: (216) 621-2234
Fax: (216) 621-4072